PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
H04L 9/00

A1

(11) International Publication Number: WO 00/65765

(43) International Publication Date: 2 November 2000 (02.11.00)

(21) International Application Number: PCT/FI00/00353

(22) International Filing Date: 25 April 2000 (25.04.00)

(30) Priority Data:
990936 26 April 1999 (26.04.99) FI

(71) Applicant (*for all designated States except US*): NOKIA NETWORKS OY [FI/FI]; P.O. Box 300, FIN-00045 Nokia Group (FI).

(72) Inventor; and
(75) Inventor/Applicant (*for US only*): HAUMONT, Serge [FR/FI]; Riistavuorenkuja 3 B 10, FIN-00320 Helsinki (FI).

(74) Agent: BERGGREN OY AB; P.O. Box 16, FIN-00101 Helsinki (FI).

(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: NEW METHOD FOR CHECKING THE DATA

(57) Abstract

This invention concerns the checking of data in a systems where the security is an important issue. According to the invention a first reference value is calculated at least partly based on a first error check value calculated from the data and a first authentication value (202). When checking the data a second error check value is calculated from the data. As well, a second reference value is calculated at least partly based on a first and a second value from the set of the second error check value, a second authentication value and the first reference value. The second reference value is compared with a third value from the set of the second error check value, the second authentication value and the first reference value. The invention also comprises a transmitter and a receiver which are arranged to perform the described operations.